Implementation and Performance Analysis of LSB Based Steganography

Prof. Arjun R. Nichal
Departement of ETC
AITRC Vita
Vita, India
arjunnichal@gmail.com

Mr. Abhinav C. Gorle
Departement of ETC
AITRC Vita
Vita, India
gorleabhinav@gmail.com

Mr. Nitin S. Chavan
Departement of ETC
AITRC Vita
Vita, India
chavan_nitin90@yahoo.in

Ms. Rohini R. Kondhalkar
Departement of ETC
AITRC Vita
Vita, India
rohinikondalkar27@gmail.com

Abstract—Protecting privacy for exchanging information through the media has been a topic researched by many people. Up to now, cryptography has always had its ultimate role in protecting the secrecy between the sender and the intended receiver. However, nowadays steganography techniques are used increasingly besides cryptography to add more protective layer to the hidden data.

Keywords*- Steganography, Data Hiding, LSB Substitution,)*

*****

I. INTRODUCTION

Information hiding in digital images has drawn much attention in recent years. Secret message encrypted and embedded in digital cover media. The redundancy of digital media as well as characteristics of human visual system makes it possible to hide secret messages. Two competing aspects are considered while designing information hiding scheme 1) Hiding capacity and 2) Imperceptibility. Hiding capacity means maximum payload. Imperceptibility means keeping undetectable. A least significant bits (LSB) substitution method is widely used for hiding data in digital images. This method widely used because of large capacity and easy implementation.

Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement is called steganography. It is the art and science of invisible communication.

The advantage of steganography over cryptography alone is that messages do not attract attention to themselves, to messengers, or to recipients. Steganographic messages are often first encrypted by some traditional means, and then a cover text is modified in some way to contain the encrypted message, resulting in stego text. This is a technique to embed additional message into some distortion-unacceptable cover media, such as military or medical images, with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message.

II. IMPLEMENTATION OF STEGANOGRAPHY METHOD

1) Image Method

In Image method we hide an image in another image. In this method we hide the data inside another image. This Purpose we use the Grayscale images as an Input and the Binary Secret image data. In this we can transmit the hidden data that is encrypted secret data inside the cover image and the receiver using the decryption method we decrypt the data and recover the secret image/data as well as the cover/input image.

1.1 Image Transmitter:

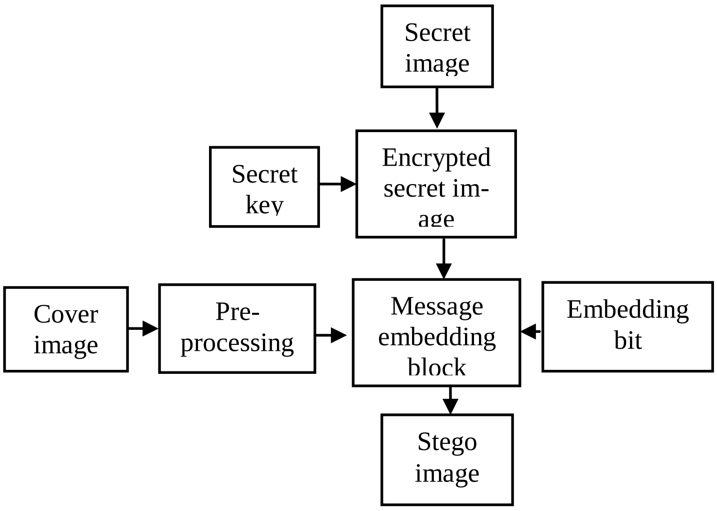


Fig1.1: Block diagram of image transmitter

Cover image:

Cover image is simply a grayscale image used for hiding our secret image/message. This images have in various formats like BMP, GIF and PNG etc. Cover image is pre-process, and the secret message/text is hide by using LSB (Least significant bit) substitution.

Pre-processing:

Before an embedding of secret message into cover image, the cover image is pre-processed for denoising an image. Image denoising is an important step in pre-processing of Images. Thresholding is applied to remove the noise without blurring edges. Gaussian filter, anisotropic PDE, wavelets are some important denoising techniques. These denoising techniques can reduce noise without destroying edges in an image. So edge information is preserved and noise is well attenuated.

Encryption method:

Image encryption is an important and effective technique to protect image security. In our project the size of secret image (binary image) is checked. After that generating key stream of same size of secret image. X⊕Ring of secret message and generated key stream will complete the encryption process.

Encrypted Image=Binary Image Keystream

Message embedding:

For embedding we used LSB (Least significant bit) substitution.

LSB (Least significant bit) substitution:

Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image. The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24-bit image, a bit of each of the red, green and blue color components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data.

Principle:

This Principle involved in this method is to replace all LSB bits of pixels of the cover image with secret bits. This method embeds the fixed length secret bits in the same fixed length LSBs of pixels. Although this technique is simple, it generally causes noticeable distortion when the number of embedded bits for each pixels exceeds three.

Advantages:

1. This method having high embedding capacity and easily implementable.

2. This method is directly replace LSBs.

1.2 Image receiver:

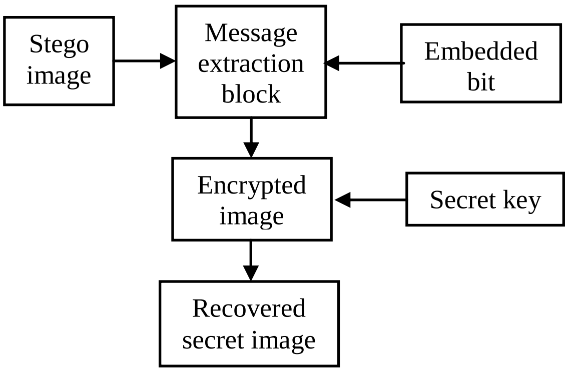


Fig1.2: Block diagram of image receiver

Stego image:

Encrypted secret image is embedded in cover image at given embedding bit position, after embedding process an image is form called stego image. Stego image contains our encrypted secret message, that message is hidden inside cover image will secure our secret message.

Extraction method:

Extraction process is opposite to embedding process. In extraction an encrypted secret message is extract from stego image from given embedding bit position. Extracted bits are in encrypted form so we can't get any secret message from this bits.

Decryption process:

From extraction we will get only encrypted message but to identify secret message decryption process is used, for decryption of secret message we require same keystream that we have used at transmitter for encryption of message. After decryption process user will get information from secret message.

2) Text Method

In Text method we Encrypt the text data in the image. In this method we hide the data inside the image. This Purpose we use the Grayscale images as an Input and the secret data is the Text file. In this we can transmit the hidden data that is encrypted secret data inside the cover image and the receiver using the decryption method we decrypt the data and recover the secret image/data as well as the cover/input image.

2.1Text Transmitter:

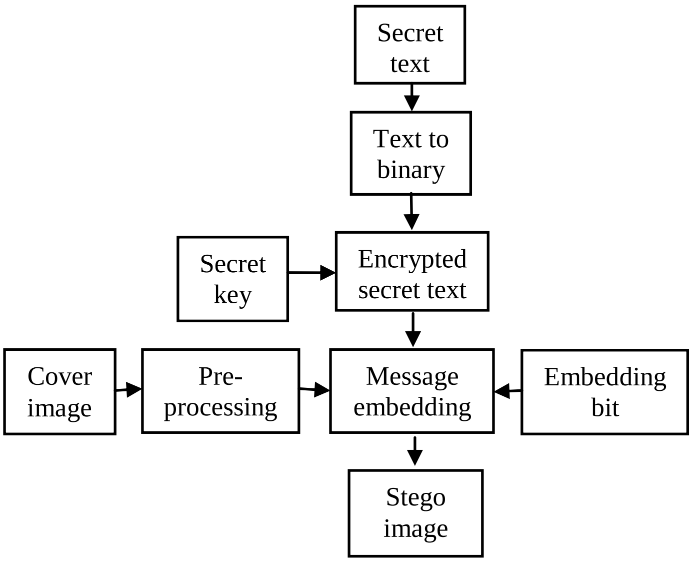


Fig1.3: Block diagram of text transmitter

The same logic is used for transmission of secret image /text.in text transmitter secret text is converted into binary then used for further processing like encryption of secret message, embedding encrypted message into cover image (grayscale image).

2.2 Text Receiver:

Message extraction block:

In message extraction process an encrypted secret message is extract from stego image, but user can't get any information from extracted message because the message is in encrypted form.

Decryption of secret message:

An encrypted secret message is decrypted using secret keystream which is used at transmitter for encryption.

Binary to text conversion:

Binary-to-text encoding is encoding of data in text. This decrypted message in binary form so user will get secret text after binary to text conversion

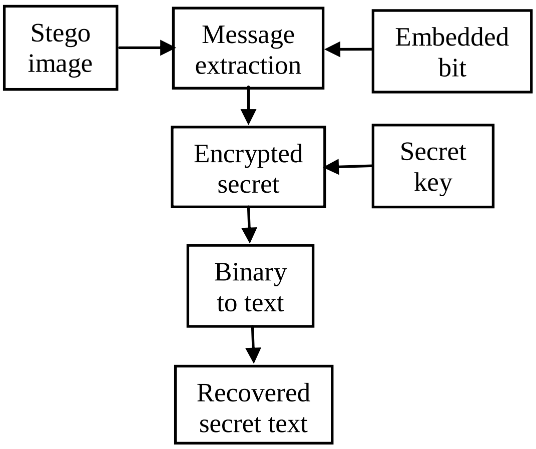


Fig1.4: Block diagram of text receiver

III. RESULTS ANALYSIS AND DISCUSSION

1) Quality Parameters

For comparing Image with Image, Image with Text, Method we have considered various quality parameters such as Compression Ratio (CR), Peak Signal to Noise Ratio (PSNR) and Embedding Capacity (EC).

1.1 Peak-Signal to Noise Ratio (PSNR)

The PSNR is most commonly used as a measure of quality of reconstruction of lossy compression codec's (e.g., for image compression). The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codec's it is used as an approximation to human perception of reconstruction quality, therefore in some cases one reconstruction may appear to be closer to the original than another, even though it has a lower PSNR (a higher PSNR would normally indicate that the reconstruction is of higher quality).

The PSNR is calculated by using following formula.

$$PSNR = 10log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

Where MAXI is maximum possible pixel value of image *I*(*i*,*j*) MSE is a mean square error. *I*(*i*,*j*)is an original cover image. *K*(*i*,*j*)is a reconstructed cover image. *m* is number of rows and *n* is number of columns.

1.2 Embedding Capacity (EC):

Embedding capacity is one of the most important quality parameter of the steganography. Embedding capacity is calculated by using following formula.

EC=*m***n*

m is number of rows and *n* is number of columns of cover image.

1.3 Number of bits Embedded (NBE):

Total pixels in Image, Total bits in Text, Total length of single stream for secret image.

For image = row*col

For Text = length of signal stream which is converted into binary from Text

2) Results:

Here same grayscale cover images are used for hiding the Images, Text inside this images. First technique consists of image method where hiding the images inside that. Second method consist of text method where hiding the text message inside the cover image. Various secret images are used for embedding.

This experiment is carried out on different class of cover images. The performance of these three techniques is compared on the basis of various quality measures such as Peak-Signal to Noise Ratio (PSNR) and Embedding Capacity (EC), Number of bits embedded (NBE).

Following results are obtained for some class of cover images. Lena image is used for hiding the data.

2.1 Image Method

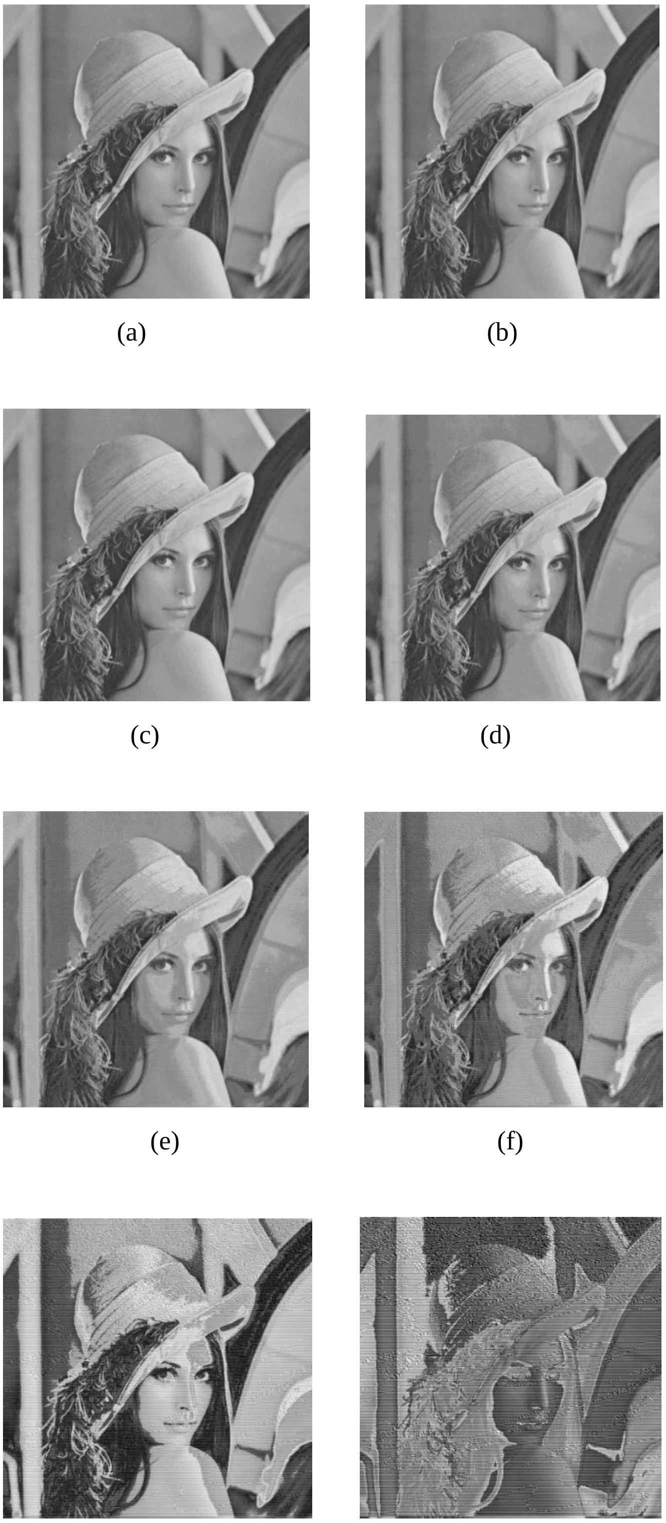
A) Following results are obtained for Lena Image with the devi image. The terms in table are EC = Embedding capacity, NBE = Number of bits embedded, PSNR = Peak signal to noise ratio.

Lena input image (512*512)

Secret image (510*510)

TABLE I. Results for Lena image with Devi Image

Embedding Bits	EC	NBE	PSNR
1	262144	260130	50.6635
2	262144	260130	44.637
3	262144	260130	38.612
4	262144	260130	32.592
5	262144	260130	26.5666
6	262144	260130	20.5496
7	262144	260130	14.5152
8	262144	260130	8.5079



(a) (b) (c) (d) (e) (f) (g) (h)

Fig1.5: Stego Images after embedding secrete image into cover image bit by bit. (1-8)

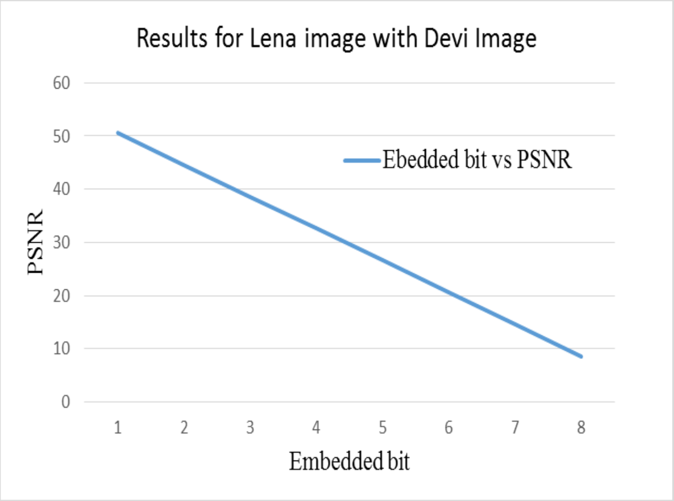
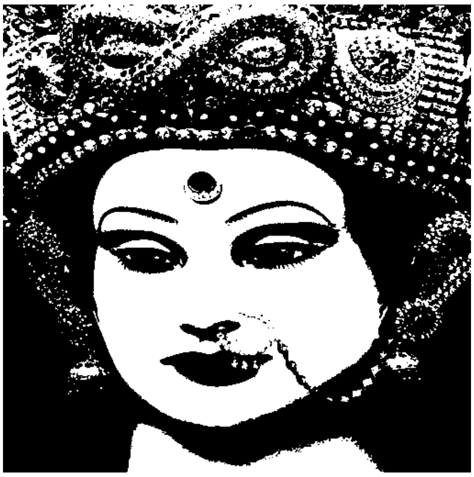


Fig1.6: Graph of Embedding bit versus PSNR for Devi image (secret image)

2.2 Text Method

The same logic is used for transmission of secret image /text.in text transmitter secret text is converted into binary then used for further processing like encryption of secret message, embedding encrypted message into cover image (grayscale image).Stego image is then transfer.

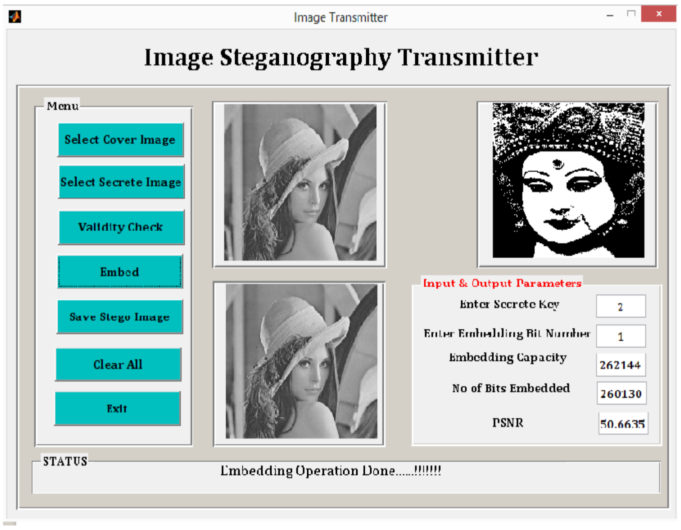
Recovered secret image at receiver:



recovered Secret image (510*510)

Graphical User Interface (GUI):

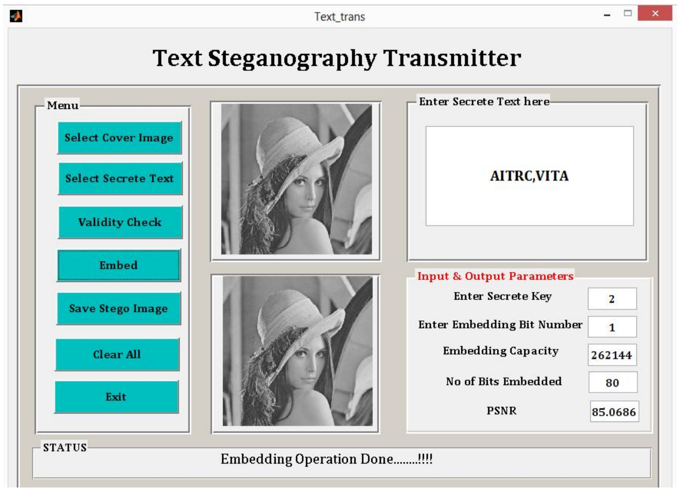
For user friendly operation graphical user interface (GUI) plays very important role.



Input & Output Parameters
Enter Secrete Key 2
Enter Embedding Bit Number 1
Embedding Capacity 262144
No of Bits Embedded 260130
PSNR 50.6635

STATUS
Embedding Operation Done......!!!!!!

Fig1.7: Image steganography transmitter



Enter Secrete Text here
AITRC,VITA

Input & Output Parameters
Enter Secrete Key 2
Enter Embedding Bit Number 1
Embedding Capacity 262144
No of Bits Embedded 80
PSNR 85.0686

STATUS
Embedding Operation Done........!!!!

Fig1.8: Text steganography transmitter

CONCLUSION

As user increases embedding bit position in cover image for hiding encrypted secret message, the Peak signal to noise ratio (PSNR) decreases linearly as well as quality of stego image decreases.

References

[1] Xinpeng Zhang "Reversible Data Hiding in Encrypted Image", IEEE SIGNAL PROCESSING LETTERS, VOL. 18, NO. 4, APRIL 2011

[2] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

[3] Z.Ni,Y.-Q.Shi,N.Ansari, andW.Su, "Reversibledata-hiding,"IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, 2006.

[4] M.U.Celik, G.Sharma, A.M.Tekalp and E.Saber, "Losslessgen-eralized-LSB data embedding,"IEEE Trans. Image Process.,vol.14, no. 2, pp. 253–266, Feb. 2005.

[5] Websites
[1] http://www.IEEE.org.in
[2]http://www.strangehorizons.com/2001/20011008/steganography

BIOGRAPHY

Prof.A.R.Nichal received his B.E. degree in Electronics and telecommunication from Shivaji University at Ashta in 2010 and received M.Tech in Electronics from Walchand College of engineering, Sangli in 2012. His area of interest is Digital Image Processing and embedded system. He published 8 International journal papers, 1 Conference paper, 1 Ebook and He has one blog on Fundamentals of Image Processing, lab Basics and Embedded System.
URL: www.imagelpcmatlab.blogspot.com

Mr. Abhinav Gorle pursuing his BE in Electronics and Telecommunication from Shivaji University at AITRC vita. His area of Interest is Image Processing and Embedded System

Mr. Nitin Chavan pursuing his BE in Electronics and Telecommunication from Shivaji University at AITRC vita. His area of Interest is Image Processing and VLSI.

Ms. Rohini kondhalkar pursuing her BE in Electronics and Telecommunication from Shivaji University at AITRC vita. Her area of Interest is Image Processing and Embedded System